## EXHIBIT C-8
## EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
## PATENT L.R. 3-3(C)

| Claim 11 ('661 Patent) | U.S. 4,932,057 to Kolbert ("Kolbert") |
|---|---|
| A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising: | 1:6-9 – "The present invention relates to data distribution, and more particularly to a distribution system for securely distributing data within an aircraft between an external source and an aircraft data system."<br>1:54-60 – "In actual utilization of the coupler described, it is impossible to completely eliminate electromagnetic radiation which might be detected by a nearby intruder, such as an enemy submarine. Accordingly, it would be highly desirable if the coupled data could be encrypted in a manner that would avoid useful decoding of the coupled data."<br>1:61-2:8 –" In my co-pending patent application Ser. No. 258,349, a random number generator, located within an aircraft, generates a random number which is coupled to the sending unit of the coupler, and from there to a data generator. This random number serves to encode the data which is ultimately transmitted, as encrypted data, to the pick-up unit, via the sending unit. Once the encrypted data is received by circuitry within the aircraft, it is decoded in the same sequence as it was encoded during encryption. Accordingly, if the random number alone or the encoded encrypted data is detected by enemy surveillance equipment, the true data itself cannot be decoded since the decoding sequence is only properly performed by compatible encoding and decoding equipment of the present invention."<br>2:15-18 – "Accordingly, it is highly desirable to effect a method for masking the internal data signals in such a manner that would prevent useful radiation detection."<br>2:26-35 – "The primary concept of the present invention is to provide the utilization devices with data subsets which are loaded in parallel so that any radiated data of each subset is masked by the other radiated superimposed subsets. More particularly, the masking occurs because each of the parallel subset paths generates a radiated signal which becomes superimposed with the other subset data which produces a resultant scrambled signal which is extremely difficult to process for retrieval of the individual data subsets." |

**Exhibit C-8 (Kolbert)**

| | |
|---|---|
| | 4:45-47, 60-64 – "Security of the described system is increased by the random number system of my co-pending patent application Ser. No. 258,349. . . .The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number." |
| (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 4:60-64 –"The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number."<br>Figure 4. |
| (b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; | 1:37-48 – "In my co-pending patent application Ser. No. 224,605, a coupling device was disclosed which preferably magnetically transfers data and circuit power to an aircraft security code storage circuit without the inclusion of mechanical pin connectors. In the environment of an aircraft, the conventional custodian's security code portable transfer box is equipped with a sending unit which is magnetically attached to the exterior of an aircraft skin At an aligned position along the interior surface of the skin is a receiving pick-up unit which magnetically picks up the digital code and low voltage power being transferred by the sending unit."<br>3:30-34 – "In operation of the device illustrated in FIG. 1, power may be supplied from the external data/power generator 10 to the internal data memory 12 in order to power the memory circuits if the aircraft power supply is turned off."<br>4:47-50 – "In operation of that system as illustrated in FIG. 4, the operational sequence generally begins after power is coupled to the internal data memory 12 as previously discussed."<br>Figure 4. |
| (c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and | 4:60-64 – "The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number."<br>Figure 4. |

| | |
|---|---|
| (d) a noise production system for introducing noise into said measurement of said power consumption. | 2:26-35 – "The primary concept of the present invention is to provide the utilization devices with data subsets which are loaded in parallel so that any radiated data of each subset is masked by the other radiated superimposed subsets. More particularly, the masking occurs because each of the parallel subset paths generates a radiated signal which becomes superimposed with the other subset data which produces a resultant scrambled signal which is extremely difficult to process for retrieval of the individual data subsets."<br>5:35-46 – "With the simultaneous parallel flow of data along cables 72, 74 and 76, any resulting radiation outside the aircraft will be detected, by unfriendly surveillance, as superimposed unintelligible signals representing the parallel distributed data subsets. In addition, the noise present along the various parallel data channels is superimposed to increase the unintelligibility of the detected signal. Shielded cables 72, 74 and 76 are typically long "spider" cables which have a tendency to radiate signals; and the present invention is directed to obviate this problem. Shielded cables 72, 74 and 76 are typically long "spider" cables which have a tendency to radiate signals; and the present invention is directed to obviate this problem."<br>Figure 5. |

| **Claim 29 ('661 Patent)** | **U.S. 4,932,057 to Kolbert** |
|---|---|
| A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising: | 1:6-9 – "The present invention relates to data distribution, and more particularly to a distribution system for securely distributing data within an aircraft between an external source and an aircraft data system."<br>1:54-60 – "In actual utilization of the coupler described, it is impossible to completely eliminate electromagnetic radiation which might be detected by a nearby intruder, such as an enemy submarine. Accordingly, it would be highly desirable if the coupled data could be encrypted in a manner that would avoid useful decoding of the coupled data."<br>1:61-2:8 –" In my co-pending patent application Ser. No. 258,349, a random number generator, located within an aircraft, generates a random number which is coupled to the sending unit of the coupler, and from there to a data generator. This random number serves to encode the data which is ultimately transmitted, as encrypted data, to the pick-up unit, via the sending unit. Once the encrypted data is |

**Exhibit C-8 (Kolbert)**

| | |
|---|---|
| | received by circuitry within the aircraft, it is decoded in the same sequence as it was encoded during encryption. Accordingly, if the random number alone or the encoded encrypted data is detected by enemy surveillance equipment, the true data itself cannot be decoded since the decoding sequence is only properly performed by compatible encoding and decoding equipment of the present invention."<br>2:15-18 – "Accordingly, it is highly desirable to effect a method for masking the internal data signals in such a manner that would prevent useful radiation detection."<br>2:26-35 – "The primary concept of the present invention is to provide the utilization devices with data subsets which are loaded in parallel so that any radiated data of each subset is masked by the other radiated superimposed subsets. More particularly, the masking occurs because each of the parallel subset paths generates a radiated signal which becomes superimposed with the other subset data which produces a resultant scrambled signal which is extremely difficult to process for retrieval of the individual data subsets."<br>4:45-47, 60-64 – "Security of the described system is increased by the random number system of my co-pending patent application Ser. No. 258,349. . . .The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number." |
| (a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; | 1:37-48 – "In my co-pending patent application Ser. No. 224,605, a coupling device was disclosed which preferably magnetically transfers data and circuit power to an aircraft security code storage circuit without the inclusion of mechanical pin connectors. In the environment of an aircraft, the conventional custodian's security code portable transfer box is equipped with a sending unit which is magnetically attached to the exterior of an aircraft skin At an aligned position along the interior surface of the skin is a receiving pick-up unit which magnetically picks up the digital code and low voltage power being transferred by the sending unit."<br>3:30-34 – "In operation of the device illustrated in FIG. 1, power may be supplied from the external data/power generator 10 to the internal data memory 12 in order to power the memory circuits if the aircraft power supply is turned off."<br>4:47-50 – "In operation of that system as illustrated in FIG. 4, the operational sequence generally begins after power is coupled to the |

| | |
|---|---|
| | internal data memory 12 as previously discussed."<br>Figure 4. |
| (b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 4:60-64 –"The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number."<br>Figure 4. |
| (c) introducing noise into said measurement of said power consumption while processing said quantity; and | 2:26-35 – "The primary concept of the present invention is to provide the utilization devices with data subsets which are loaded in parallel so that any radiated data of each subset is masked by the other radiated superimposed subsets. More particularly, the masking occurs because each of the parallel subset paths generates a radiated signal which becomes superimposed with the other subset data which produces a resultant scrambled signal which is extremely difficult to process for retrieval of the individual data subsets."<br>5:35-46 – ""With the simultaneous parallel flow of data along cables 72, 74 and 76, any resulting radiation outside the aircraft will be detected, by unfriendly surveillance, as superimposed unintelligible signals representing the parallel distributed data subsets. In addition, the noise present along the various parallel data channels is superimposed to increase the unintelligibility of the detected signal. Shielded cables 72, 74 and 76 are typically long "spider" cables which have a tendency to radiate signals; and the present invention is directed to obviate this problem."<br>Figure 5. |
| (d) outputting said cryptographically processed quantity to a recipient thereof. | 4:52-5:7 – "A random number generator 51 located within the aircraft generates a random number and outputs it to the pick-up unit 19. Since the pick-up unit and sending unit are symmetrical and inductively coupled devices, the pick-up unit acts as a primary at this time, while the sending unit 14 acts as a secondary. The random number becomes stored in buffer 52 which is located in the data generator 10. The data stored in memory 55 and the random number are encoded in an encoder 54 in accordance with a specific sequence. The encoded data now represents an encryption of the basic data by the random number. Wire 13 connects the output of encoder 54 to the sending unit 14 so that the encoded data may be coupled to the pick-up unit 19. The latter unit then outputs the encoded data to buffer 56 within the aircraft. A decoder 58 has its |

**Exhibit C-8 (Kolbert)**

| | |
|---|---|
| | inputs 60, 62 respectively connected to the random number generator and the encoded data buffer so that the encrypted data may be decoded in accordance with the same specific sequence governing the encoder 54. The output 64 of the decoder then delivers the decoded data to the internal data memory 12 for use by other data or communication equipment on board the aircraft in a conventional fashion." |